Expert Report on Cryptocurrency Losses: Analysis of Suspected Trojan Horse Applications, iPhone Logs, and Law Enforcement Challenges

Executive Summary

This report addresses significant concerns regarding extensive cryptocurrency losses experienced over several years, attributed by the user to the presence of 721 identified "Trojan Horse applications" on a laptop. Additionally, the report considers the potential involvement of an iPhone and the perceived lack of assistance from Dutch law enforcement.
The analysis confirms that the identified list of malware encompasses numerous types explicitly designed to target cryptocurrency, financial credentials, and system resources. This strongly suggests a high likelihood of direct financial impact from these infections. While a direct assessment of the provided iPhone logs was not possible due to technical limitations, the general risks associated with mobile malware and the potential for cross-device compromise are discussed, highlighting the importance of comprehensive security across all digital assets.
Challenges faced by law enforcement in investigating cryptocurrency fraud are systemic, stemming from the global and decentralized nature of digital assets, jurisdictional complexities, and technical resource gaps. These factors often contribute to the perception of limited assistance or difficulty in recovering stolen funds. Furthermore, it is crucial to recognize that cryptocurrency losses frequently stem from sophisticated non-malware-related fraud vectors, such as investment scams and phishing attacks, which often exploit human vulnerabilities rather than technical ones.
Immediate recommendations include isolating all potentially compromised devices and seeking professional cybersecurity forensic analysis and system re-imaging. Long-term security for digital assets necessitates rigorous adherence to best practices in secure wallet management, robust authentication, and continuous vigilance against social engineering. It is also important to maintain realistic expectations regarding the recovery of stolen cryptocurrency and to understand the various avenues for reporting cybercrime.

1. Introduction: Understanding the User's Situation

The user, Sergio Fernando Baptista, has reported a distressing situation involving the discovery of 721 "Trojan Horse applications" on a laptop. This substantial number of malicious programs is believed to be the underlying cause of significant cryptocurrency losses incurred over a period of several years. The user has also expressed frustration regarding the perceived inability of law enforcement in the Netherlands to provide effective assistance in addressing these losses. In addition to the laptop, recent iPhone logs (from an iPhone 12,1 running iOS 18.5) were provided, indicating a concern about potential related issues on the mobile device.
This report aims to provide a comprehensive analysis of the situation. It will delve into the technical mechanisms by which the identified malware could have led to cryptocurrency theft,

evaluate the general security posture of mobile devices in such contexts, and explore the systemic challenges that law enforcement agencies, particularly in the Netherlands, face when investigating complex, cross-border cryptocurrency fraud. Furthermore, the report will examine alternative explanations for cryptocurrency losses that extend beyond direct malware infection, offering a broader perspective on the potential causes of the financial impact.

2. Analysis of Identified Trojan Horse Applications and Cryptocurrency Loss Mechanisms

The extensive list of 721 "Trojan Horse applications" provided by the user represents a diverse array of malware families. These are categorized by their primary execution environment or file type, including AndroidOS, ASP, BAT, DOS, HTA, IRC, Java, JS, LNK, MacOS, MSIL, PDF, PowerShell, Python, Script, SH, VBA, VBS, W97M, Win16, Win32, Win64, WinNT, WM, X97M, XF, and XML. Many of these categories and specific malware names are well-known in the cybersecurity community for their direct association with financial crime, information theft, and the targeting of cryptocurrency assets.

The sheer diversity and volume of malware identified on the user's system indicate a prolonged and multi-vector attack surface. The presence of such a comprehensive catalog, spanning various operating systems (Android, MacOS, Windows), scripting languages (JS, PowerShell, Python, VBS), and document types (PDF, W97M, XML), strongly suggests that the user's system has been exposed to numerous infection vectors over an extended period. This could have occurred through compromised websites, malicious email attachments, pirated software, or even sophisticated supply chain attacks. The inclusion of both older threats, such as variants of the Zeus banking Trojan like Zloader, and more contemporary threats like Lumma Stealer, which has been active since at least 2022, lends significant credibility to the user's claim of "years of cryptocurrency losses". This long-term presence points to a persistent compromise rather than an isolated incident, making comprehensive remediation particularly challenging due to the potential for multiple backdoors and persistence mechanisms.

Furthermore, the presence of various "Loader" malware types, including Win32/Loader, MSIL/CobaltStrikeLoader, Win32/CobaltLoader, Win64/CobaltStrikeLoader, Win32/AnchorLoader, Win32/Banload, Win64/Banload, Win32/DarkGateLoader, PowerShell/DarkgateLoader, Win32/MofngoLoader, MSIL/CoinMinerLoader, MSIL/CobaltStrikeLoader, Win64/CobaltStrikeLoader, Win64/BazaarLoader, Win64/BazaLoder, Win64/Bazarldr, Win64/BazarldrCrypt, and Win64/Bazzarldr, implies a dynamic and evolving threat landscape on the user's system. Loader malware is specifically designed to deliver and execute *additional* malicious payloads. This means that the 721 identified applications may not represent the final, directly impactful malware, but rather a collection of initial access tools, droppers, and the subsequent, more potent malware they installed. For example, Emotet is frequently observed loading TrickBot, which can then proceed to deploy Ryuk ransomware. Similarly, IcedID has been documented as an entry point for more sophisticated attacks, including human-operated ransomware and the deployment of Cobalt Strike. This layered attack strategy suggests that initial infections enabled further, more targeted attacks, potentially escalating the financial impact over time. The user's system likely served as a persistent entry point for various financially motivated cybercriminal groups, continuously exposing their assets to new and evolving threats.

The extensive list of malware, coupled with their known persistence and evasion techniques, strongly supports the user's assertion of "years of cryptocurrency losses." It is highly improbable

for 721 distinct malware instances to appear simultaneously. Instead, this suggests a cumulative effect of numerous, possibly overlapping, infection campaigns. Malware families like Emotet and TrickBot are notorious for their longevity and their ability to continuously evolve and deliver new threats. The presence of "loaders" further reinforces this, as they provide a continuous foothold for threat actors to deploy new or updated malicious payloads over time, adapting to new cryptocurrency trends or security measures. This indicates that the user's system likely remained a lucrative target for various cybercriminal groups for an extended period.
A particularly concerning aspect is the presence of sophisticated post-exploitation frameworks like Cobalt Strike. This suggests that the compromised system was not merely a victim of automated attacks but potentially a target for human-operated intrusions. Cobalt Strike is a commercial red-teaming tool widely abused by advanced threat actors for post-exploitation activities, including data exfiltration, lateral movement within a network, and deploying final payloads like ransomware. Its use implies a higher level of attacker sophistication, potentially involving manual exploration of the compromised network to identify high-value assets, such as cryptocurrency wallets or exchange access, and then orchestrating targeted theft. This elevates the nature of the threat beyond simple automated malware infections to a more deliberate and potentially devastating campaign.

2.1. Common Malware Types and Their Cryptocurrency Loss Mechanisms

The following table details several prominent malware types identified in the provided list and explains their specific mechanisms for causing cryptocurrency losses.

Malware Name (Examples from list)	Primary Category	Key Functionality	Method of Cryptocurrency Loss	Relevant Snippet IDs
Lumma Stealer (JS/LummaStealer, MSIL/LummaStealer, PowerShell/LummaStealer, Script/LummaStealer, Win32/LummaStealer, Win64/LummaStealer)	Infostealer	Steals credentials, banking info, and cryptocurrency wallets.	Direct theft of private keys, seed phrases, and login credentials for online exchanges or software wallets.	
CoinMiner (BAT/CoinMiner, PowerShell/CoinMiner, Win32/CoinMiner)	Cryptojacker	Uses system resources (CPU, GPU, RAM) to mine cryptocurrency for attackers; often drops clipper malware.	Theft of computing resources and electricity, leading to higher bills, system slowdowns, and hardware strain.	

Malware Name (Examples from list)	Primary Category	Key Functionality	Method of Cryptocurrency Loss	Relevant Snippet IDs
Emotet (JS/Emotet, MSIL/Emotet, PDF/Emotet, PowerShell/Emotet, Script/Emotet, VBA/Emote, VBS/Emotet, W97M/Emotet, Win32/Emotet, Win64/Emotet, X97M/Emotet, XF/Emotet, XML/Emotet)	Banking Trojan/Loader	Steals financial data, email credentials, spreads laterally, downloads other malware (e.g., TrickBot, ransomware).	Steals credentials for cryptocurrency exchanges/wallets, intercepts SMS for 2FA bypass, or facilitates further malware leading to crypto loss.	
TrickBot (BAT/TrickBot, JS/TrickBot, MSIL/TrickBot, PowerShell/TrickBot, VBS/TrickBot, Win32/TrickBot, Win64/Trickbot, Win64/TrickBotCrypt)	Banking Trojan/Infostealer/ Loader	Steals financial data, credentials, can cryptomine, installs ransomware (Ryuk, Conti), spreads laterally.	Steals financial data and credentials for crypto accounts; can directly cryptomine on the victim's system or deploy ransomware.	
QakBot (BAT/Qakbot, HTA/Qakbot, JS/Qakbot, MSIL/Qakbot, PDF/Qakbot, PowerShell/QakBot, Script/Qakbot, VBS/Qakbot, Win32/QakBot, Win64/QakBot, X97M/Qakbot)	Banking Trojan/Loader	Steals financial info, propagates, delivers ransomware (Conti, REvil, Prolocked, Black Basta, Cactus), harvests email credentials.	Steals financial information for crypto accounts; acts as a delivery mechanism for ransomware that encrypts files and demands crypto ransom.	
Zloader (BAT/Zloader, JS/Zloader, MSIL/Zloader, PowerShell/ZLoader, VBS/Zloader, Win32/Zloader, Win64/Zload,	Banking Trojan/Loader	Steals cookies, passwords, sensitive info, provides VNC access, loads Cobalt Strike and ransomware (Egregor, Ryuk).	Steals credentials for crypto accounts, provides remote access for manual theft, or deploys ransomware leading to crypto	

Malware Name (Examples from list)	Primary Category	Key Functionality	Method of Cryptocurrency Loss	Relevant Snippet IDs
Win64/ZLoader, Win64/ZLoaderE)			loss.	
WannaCrypt (MSIL/WannaCrypt, VBS/WannaCrypt, Win32/WannaCrypt, Win64/WannaCrypt)	Ransomware	Encrypts files and demands Bitcoin ransom; spreads as a worm.	Direct financial loss if the victim pays the ransom; loss of access to data, including potentially crypto wallets or related files, if not paid.	
DCRAT (MSIL/DCRAT, PowerShell/DCRat, Python/DCRat, Win32/DCRAT, Win64/DCRat)	Remote Access Trojan (RAT)	Performs various malicious actions; can be used for crypto ransomware.	Can be used to steal credentials, install other crypto-targeting malware, or encrypt files for ransom.	
IcedID (BAT/IcedID, HTA/IcedID, JS/IcedID, MSIL/IcedID, PDF/IcedID, PowerShell/IcedID, Python/IcedId, Script/IcedID, VBS/IcedID, W97M/IcedId, Win32/IcedId, Win64/IcedID)	Banking Trojan/Dropper	Steals financial info via man-in-the-middle or browser injects; acts as entry point for human-operated ransomware and Cobalt Strike.	Steals credentials for crypto accounts or facilitates the deployment of ransomware and other data-exfiltration tools.	
CobaltStrike (BAT/CobaltStrike, Java/CobaltStrike, JS/CobaltStrike, MacOS/CobaltStrike, MSIL/CobaltStrike, PowerShell/CobaltStrike, Script/CobaltStrike, VBS/CobaltStrike, Win32/CobaltSTrike,	Post-exploitation Framework	Used by threat actors to simulate attacks, deploy payloads (Beacon), exfiltrate data, bypass 2FA.	Enables attackers to gain deep access to systems, steal credentials, bypass security measures, and exfiltrate cryptocurrency or related data.	

Malware Name (Examples from list)	Primary Category	Key Functionality	Method of Cryptocurrency Loss	Relevant Snippet IDs
Win64/CobaltStrike, XML/CobaltStrike)				
AndroidOS/Banker (AndroidOS/Banker)	Banking Trojan/Infostealer	Targets mobile banking/social media apps, intercepts SMS (2FA bypass), steals recovery phrases via OCR, extracts personal info from screenshots.	Steals mobile banking credentials, intercepts SMS messages for 2FA bypass, and can directly extract cryptocurrency recovery phrases from images.	

2.2. Direct Mechanisms of Cryptocurrency Loss

The various malware families identified on the user's system employ several direct mechanisms to cause cryptocurrency losses:

Information Stealers (Infostealers): These malware types are specifically engineered to harvest sensitive data from compromised systems. Lumma Stealer, for example, is a Malware-as-a-Service (MaaS) offering widely used by financially motivated threat actors. It is highly capable of stealing data from various browsers and applications, with a particular focus on "cryptocurrency wallets". Similarly, IcedID, which originated as a banking trojan in 2017, has evolved to steal credentials through sophisticated man-in-the-middle techniques or browser injects. Zloader also possesses the capability to steal cookies, passwords, and other sensitive information. A more recent threat, StilachiRAT, explicitly scans the Google Chrome browser for over 20 crypto wallet extensions and extracts saved browser credentials, actively monitoring clipboard activity for passwords or crypto keys. The direct impact of these infostealers on cryptocurrency holdings is the theft of private keys, seed phrases, and login credentials for online exchanges or software wallets. Once these critical pieces of information are compromised, attackers gain full, irreversible control over the victim's funds, allowing them to drain wallets without authorization.

Clipper Malware: This specialized type of malware, exemplified by MassJacker or the clipper component often dropped by Coinminer, operates by monitoring the victim's clipboard—the temporary storage area for copied data. When a cryptocurrency wallet address is copied by the user, the malware swiftly intercepts this action and replaces the legitimate address with an attacker-controlled address. The consequence is that unsuspecting users, believing they are pasting their intended recipient's address, inadvertently paste the attacker's address instead. This redirection of transactions leads to irreversible financial loss, as the funds are sent directly to the cybercriminal's wallet.

Cryptojacking/Coinmining: Malware such as BAT/CoinMiner infiltrates a computer system and surreptitiously utilizes its hardware resources, including the CPU, GPU, and RAM, to mine cryptocurrency for the attacker without the user's knowledge or consent. TrickBot is also known to possess cryptomining capabilities. These operations often employ stealth techniques, such as mining only during specific hours or disabling security software, to remain undetected for as

long as possible. While cryptojacking does not involve the direct theft of existing cryptocurrency from a wallet, it constitutes a significant theft of computing resources and electricity. This can manifest as "elevated electricity bills," "unexplained slowdowns" in system performance, "increased system heat," and "unusual network activity". Over time, the cumulative cost of wasted resources and potential hardware degradation can represent a substantial financial burden.

Ransomware: Ransomware variants, including WannaCrypt and Win32/Snake, operate by encrypting files on the victim's device, rendering them inaccessible. Following encryption, a ransom note is displayed, typically demanding payment in cryptocurrency, most commonly Bitcoin, in exchange for the decryption key. DCRAT also has the capability to be used for crypto ransomware. The primary financial impact here is the direct loss incurred if the victim chooses to pay the ransom, with no guarantee that the decryption key will be provided or that files will be fully recovered. Even without paying the ransom, the user suffers the loss of access to their data, which may include critical files related to cryptocurrency wallets or other financial information. Ransomware often attempts to prevent recovery by deleting shadow volume copies of operating systems.

Banking Trojans: Originally designed to compromise traditional financial data, banking Trojans like Emotet, TrickBot, QakBot, Zloader, and AndroidOS/Banker have expanded their capabilities to target cryptocurrency. These malware types intercept online banking credentials, e-payment system data, and plastic card information. They often employ sophisticated techniques such as displaying fake login screens or executing man-in-the-browser attacks to trick users into divulging sensitive information. The relevance to cryptocurrency lies in their ability to steal credentials for cryptocurrency exchanges and online wallets, or to intercept critical SMS messages used for two-factor authentication (2FA). This allows attackers to bypass security measures and drain accounts. Some advanced variants, like AndroidOS/Banker (specifically the SparkCat variant), even utilize Optical Character Recognition (OCR) to identify and steal cryptocurrency recovery phrases found in screenshots or images stored on a device.

Remote Access Trojans (RATs): RATs, such as StilachiRAT, provide cybercriminals with comprehensive remote control over an infected device. This level of access enables attackers to exfiltrate sensitive data, manipulate system settings, install additional malware, and establish persistent access. In the context of cryptocurrency, RATs can be used to directly access and drain crypto wallets, steal private keys, monitor clipboard activity for crypto-related data, and gather system information that could facilitate further, more targeted attacks. Their built-in evasion and anti-forensics mechanisms, such as clearing event logs and detecting sandbox environments, make them particularly challenging to detect and remove.

Loader Malware: As previously discussed, loaders serve as initial infection vectors, primarily designed to deliver and execute secondary payloads. Many of the Trojans identified in the user's list, including Emotet, TrickBot, QakBot, IcedID, and Zloader, function as sophisticated loaders. They establish persistence and command-and-control (C2) communication channels to download and deploy more potent malware. While loaders do not directly steal cryptocurrency, they are critical enablers for other crypto-targeting malware, such as ransomware, info-stealers, and RATs. Their pervasive presence signifies a deeply compromised system that acts as a gateway for a continuous stream of various financially motivated attacks. This continuous compromise provides a compelling explanation for the user's claim of "years of cryptocurrency losses," as new threats could be deployed and updated over time, adapting to new cryptocurrency trends or security measures.

2.3. The Scale and Persistence of the Infection

The identification of 721 "Trojan Horse applications" is an extraordinarily high number, which strongly suggests a deeply compromised system. Many of the identified malware types, including Emotet, TrickBot, QakBot, Zloader, and Cobalt Strike, are renowned for their sophisticated persistence mechanisms. These mechanisms include the creation of auto-start registry keys, scheduled tasks, and Windows services, ensuring that the malware re-executes even after system reboots. Furthermore, these malware families often possess lateral movement capabilities, enabling them to spread across networks, frequently by abusing the Server Message Block (SMB) protocol. Their ability to evade detection is also a hallmark, achieved through polymorphism, anti-analysis features, and even by disabling legitimate security software.

The extensive list of malware, combined with their known persistence and evasion techniques, strongly corroborates the user's claim of "years of cryptocurrency losses." It is highly improbable for 721 distinct malware instances to appear simultaneously. Instead, this indicates a cumulative effect of numerous, possibly overlapping, infection campaigns over an extended period. Malware like Emotet and TrickBot are known for their longevity and their ability to continuously evolve and deliver new threats. The presence of "loaders" further supports this, as they provide a continuous foothold for threat actors to deploy new or updated malicious payloads over time, adapting to new cryptocurrency trends or security measures. This means the user's system likely remained a lucrative target for various cybercriminal groups for an extended period, leading to ongoing financial depletion.

The presence of sophisticated post-exploitation frameworks like Cobalt Strike suggests that the compromised system was not merely a victim of automated attacks but potentially a target for human-operated intrusions. Cobalt Strike is a commercial red-teaming tool widely abused by advanced threat actors for post-exploitation activities, including data exfiltration, lateral movement, and deploying final payloads like ransomware. Its use implies a higher level of attacker sophistication, potentially involving manual exploration of the compromised network to identify high-value assets, such as cryptocurrency wallets or exchange access. This manual intervention allows for a more tailored and effective attack, where threat actors can adapt their methods based on what they discover on the system. This elevates the nature of the threat beyond simple automated malware infections to a more deliberate and potentially devastating campaign, explaining how losses could accumulate over a long duration as attackers systematically exploited the access gained.

3. Assessment of iPhone Logs and Mobile Device Security

3.1. Limitations of iPhone Log Analysis

It is important to state that a direct analysis of the provided iPhone logs was not possible. This is a common limitation when dealing with private or locally stored data, or due to inherent security protocols that prevent external access to sensitive user information. This technical inability to review the specific logs means that a direct forensic assessment of the iPhone's network activity, device information, or any specific indicators of compromise cannot be provided within

this report.

3.2. Potential for iOS Malware and Cross-Device Infection

Despite the inability to review the specific logs, it is crucial to discuss the general risks to iOS devices and the potential for cross-device infection, as the user's concern about the iPhone's involvement is valid. While often perceived as more secure, iOS devices are not immune to malware. For instance, Kaspersky identified "SparkCat," detected as HEUR:Trojan.IphoneOS, which was found in the AppStore. This particular malware variant is notable for its use of Optical Character Recognition (OCR) to identify and steal cryptocurrency wallet recovery phrases from screenshots stored in a user's photo gallery.

Furthermore, mobile banking Trojans, such as BankBot/Spy Banker (an AndroidOS/Banker variant), are capable of intercepting SMS messages. This functionality is critically important in the context of cryptocurrency security, as SMS is frequently used for two-factor authentication (2FA) on banking or crypto accounts. By intercepting these messages, attackers can bypass a crucial layer of security, gaining unauthorized access to accounts even if they do not possess the primary password.

The potential for cross-device compromise is a significant threat vector that must be considered. If the user stored cryptocurrency wallet recovery phrases, private keys, or other sensitive credentials as screenshots or notes on their iPhone, these could be vulnerable to mobile-specific malware like SparkCat. Additionally, if the iPhone was used to access compromised online accounts or websites, or if it was physically connected to the infected laptop for data transfer or syncing, a pathway for malware propagation or credential theft could have been established. Moreover, if credentials (passwords, 2FA codes) were synced across devices via cloud services or password managers, a compromise on one device could inevitably affect the security of the other.

Even without direct access to the iPhone logs, the user's concern about the iPhone's involvement is valid, as mobile devices are increasingly targeted for crypto theft, and cross-device compromise is a significant threat vector. The user explicitly provided iPhone logs, indicating a suspicion of its involvement. While the laptop is clearly deeply compromised, modern cyberattacks frequently span multiple devices. The existence of iOS-specific crypto-stealing malware like SparkCat and the general capabilities of mobile banking Trojans demonstrate that iPhones are not immune to sophisticated attacks. Furthermore, poor security hygiene, such as storing seed phrases digitally on a phone or syncing credentials across devices, creates a direct bridge for attackers to move from a compromised laptop to a mobile device, or vice-versa, to access cryptocurrency assets. This interconnectedness underscores the critical need for a holistic security approach that encompasses all digital devices used for cryptocurrency management.

4. Challenges with Law Enforcement Assistance in the Netherlands

The user's experience with law enforcement in the Netherlands, specifically the perceived lack of assistance, reflects systemic challenges inherent in investigating and prosecuting cryptocurrency-related crimes. These challenges are multifaceted, encompassing jurisdictional complexities, technical and resource limitations, and the specific mandates of financial

intelligence units.

4.1. Jurisdictional Complexities and Cross-Border Cybercrime

Cryptocurrency crime is inherently global, transcending national borders and jurisdictions. Criminal networks adeptly exploit these geographical and legal boundaries, operating across multiple countries to evade detection and prosecution. This international dimension means that data and evidence relevant to an investigation are often "scattered across multiple platforms, jurisdictions, and agencies," significantly complicating efforts to piece together a coherent case. A major hurdle is the use of anonymization services by criminals, such as mixers and privacy coins, which are designed to obfuscate transaction trails and make the tracing of illicit funds exceedingly difficult. These services intentionally blend legitimate and illicit funds, making it nearly impossible for investigators to follow the money. The global, decentralized nature of cryptocurrency, combined with these sophisticated obfuscation techniques, creates a significant "jurisdictional void" that law enforcement struggles to bridge, often leading to the user's perceived lack of assistance. Unlike traditional banking systems where transactions can often be disputed or reversed, crypto transactions are irreversible and frequently cross numerous borders instantly. This makes freezing funds or pursuing perpetrators incredibly difficult, especially when they operate from countries with weak extradition treaties or where cybercrime is state-sponsored, as seen with North Korea's significant role in crypto theft. The sentiment of "we have no law for your crime" accurately captures a real challenge in this rapidly evolving legal landscape, where existing frameworks struggle to keep pace with technological advancements and criminal ingenuity.

4.2. Technical and Resource Limitations of Law Enforcement

Many law enforcement agencies (LEAs) globally, including those in the Netherlands, face significant technical and resource limitations that hinder their ability to effectively combat cryptocurrency crime. A primary issue is the widespread "lack of expertise needed to understand blockchain technology, analyze transactions, and interpret cryptocurrency data". This knowledge gap extends to a struggle to "hire and retain specialized expertise – such as data scientists, digital forensics and other experts" , who are crucial for navigating the complexities of digital investigations.

Furthermore, LEAs often lack the necessary "information technology (IT) (software and hardware) and capacity-building resources for training staff" required to handle the "massive volumes of data" involved in cybercrime investigations. The rapid evolution of crypto technology and cybercrime tactics consistently outpaces the institutional capacity-building of many law enforcement agencies, creating a persistent gap in their ability to effectively respond to complex crypto fraud cases. While specialized blockchain analytics solutions like Chainalysis exist and are used by some law enforcement entities , widespread adoption and comprehensive training across all agencies are often slow. The constant need for software updates, patch fixes, and understanding new malware variants means that even if LEAs acquire advanced tools, the human expertise required to wield them effectively against ever-evolving threats is a continuous challenge. This directly impacts their ability to provide the kind of in-depth investigative support a victim might expect for a multi-year, multi-malware crypto loss scenario.

4.3. Role of Financial Intelligence Units (FIUs)

The Financial Intelligence Unit-The Netherlands (FIU-NL) serves as the central agency responsible for collecting, analyzing, and disseminating financial intelligence to combat money laundering, terrorist financing, and other financial crimes within the Netherlands. FIU-NL receives suspicious transaction reports from various obligated entities, such as banks, financial institutions, and professional crypto service providers, and subsequently shares this intelligence with law enforcement agencies.
However, a critical limitation of the FIU-NL, as noted in the provided information, is that it "has no investigative power". Its mandate primarily focuses on anti-money laundering (AML) and counter-terrorism financing (CTF) policy development and intelligence sharing, rather than direct victim assistance or the recovery of stolen funds. While FIUs like FIU-NL are crucial in the broader fight against financial crime, their mandate and operational model mean they are not equipped to directly assist individual victims in recovering stolen cryptocurrency, which contributes to the user's frustration. The user's query is about personal financial loss and the perceived lack of direct help. FIU-NL's role is at a macro-level: identifying patterns, trends, and connections for broader law enforcement efforts. This structural separation means that even if a crime is reported and falls within their purview for intelligence gathering, it does not translate into immediate, tangible help for the individual victim, creating a significant disconnect between public expectations and institutional capabilities.

4.4. Data Retention and Information Sharing Issues

Europol and Eurojust reports highlight "data loss" as a common and significant challenge in cybercrime investigations. This issue is largely due to the invalidation of the Data Retention Directive, which has led to inconsistent or non-existent data retention periods across various EU Member States. Consequently, crucial digital evidence, such as IP logs or transaction details, might not be available by the time a crime is discovered, especially if days or weeks have passed since the incident.
Furthermore, "obstacles to international cooperation" and challenges in "public-private partnerships" (e.g., data-sharing restrictions, the sensitive nature of investigations) further complicate the fight against cybercrime that often spans multiple jurisdictions. The ephemeral nature of digital evidence, exacerbated by inconsistent data retention laws and international cooperation hurdles, creates a "cold case" problem for cybercrime investigations, making the recovery of multi-year losses exceptionally difficult. Cryptocurrency transactions are inherently fast and irreversible. If critical data is not retained by service providers for sufficient periods, or if there are legal barriers to sharing it across borders, the digital trail quickly goes cold. For "years of cryptocurrency losses," much of the crucial digital evidence may have already been purged or become inaccessible due to these systemic issues, rendering a successful investigation and recovery increasingly improbable over time. This underscores the profound difficulties faced by law enforcement in providing direct assistance to victims of long-term, complex cryptocurrency theft.

5. Alternative Explanations for Cryptocurrency Losses (Beyond Direct Malware)

While the presence of 721 Trojan Horse applications on the user's laptop strongly indicates a significant malware-related compromise, it is crucial to consider that cryptocurrency losses can also stem from a variety of other, non-malware-related factors. These alternative explanations,

often rooted in social engineering and systemic vulnerabilities, are highly prevalent in the crypto space and may have contributed to, or even been the primary cause of, the reported multi-year losses.

5.1. Investment Scams and Fraud

Investment scams and fraud represent a leading cause of cryptocurrency losses. In 2023, the majority of cryptocurrency losses (71%) were attributed to investment fraud. In 2024, high-yield investment scams and "pig butchering" scams, which blend romance scams with investment fraud, were identified as the most successful types.
These scams employ various deceptive methods:

- Scammers create "fake websites mimicking real exchanges or wallets," designed to appear legitimate but serving to steal funds.
- They promise "guaranteed profits or big returns" that are unrealistic and unattainable.
- Impersonation is common, with scammers posing as "celebrities" or influential figures to lure potential victims.
- "Giveaway scams" promise to multiply cryptocurrency sent to them, creating a false sense of urgency and legitimacy.
- Scammers frequently use social media platforms or dating apps to build trust with victims before introducing the fraudulent investment opportunity.
- Victims are often tricked into depositing funds onto fraudulent platforms from which they are later unable to withdraw their money, with scammers providing excuses or demanding additional fees before ultimately shutting down the platform.

The direct impact of these scams is the irreversible loss of invested cryptocurrency, often in significant amounts, as funds are transferred directly to attacker-controlled wallets. The user's multi-year losses, while potentially linked to malware, could also be significantly influenced by, or even primarily caused by, sophisticated social engineering and investment scams, which are the leading cause of crypto losses. While malware can steal credentials that enable these scams, the scams themselves frequently rely on psychological manipulation rather than purely technical exploits. It is plausible that the user was simultaneously battling malware *and* falling victim to these pervasive scams, or that an initial malware infection facilitated access that then led to social engineering attempts. This broader perspective suggests a need to investigate beyond just technical compromise.

5.2. Phishing Attacks and Social Engineering

Phishing attacks and social engineering are pervasive threats in the cryptocurrency space. Attackers impersonate "trusted platforms or wallets" through various channels, including "fake websites" , "scam emails or DMs" , or "malicious browser extensions". The objective is to trick users into revealing sensitive information such as "private keys, seed phrases, or passwords". Phishing sites accounted for 8% of all observed malicious sites in the first half of 2024.
The direct impact of phishing is the immediate theft of funds once attackers gain unauthorized access to wallets or exchange accounts using the stolen credentials. These cryptocurrency transactions, once executed, are irreversible. Phishing and social engineering are often intertwined with malware infections, acting as the initial access vector or a secondary exploitation method, making it difficult to isolate a single cause for the user's losses. Many malware types, including Emotet, TrickBot, IcedID, and Zloader, are primarily spread via "malspam" or "phishing campaigns". This means the user's extensive malware infection likely

began with a successful phishing attempt. Conversely, even after malware has established a presence on a system, attackers might leverage social engineering tactics to trick the user into making direct transfers or revealing additional credentials, effectively bypassing technical security measures. This creates a complex attack chain where the ultimate "cause" of loss is not solely the malware itself, but the human element exploited via social engineering.

5.3. Insecure Cryptocurrency Exchange Practices

Beyond individual device compromises, systemic vulnerabilities within the broader cryptocurrency ecosystem can also lead to significant losses. Cryptocurrency exchanges are "lucrative targets for hackers" , with billions of dollars stolen annually due to "security vulnerabilities" within their platforms. Notable examples of major exchange hacks include Mt. Gox, FTX, Binance, and the Ronin Network.

A common vulnerability arises from storing assets in "hot wallets" (internet-connected wallets) rather than more secure "cold wallets" (offline storage), which significantly increases exposure to attacks. Another sophisticated attack vector is SIM swap attacks, where attackers compromise a user's phone by persuading service providers to transfer the phone number to their own SIM card. This allows them to bypass multi-factor authentication (MFA) and reset passwords, thereby gaining access to crypto accounts. Furthermore, insufficient use of two-factor authentication (2FA) or multi-factor authentication (MFA) by users leaves accounts vulnerable even if primary passwords are stolen.

While malware can compromise individual devices, systemic vulnerabilities within the broader cryptocurrency ecosystem, particularly insecure exchange practices and insufficient user security habits, can lead to significant losses regardless of direct device infection. The user's losses could stem from vulnerabilities at the exchange level (e.g., an exchange hack impacting their funds) or from their own practices on these platforms (e.g., not using 2FA, keeping large amounts in hot wallets). A SIM swap attack, for instance, directly targets the user's phone number to bypass security on exchanges, not necessarily their laptop. This means that even a perfectly clean laptop might not prevent cryptocurrency loss if the exchange itself is compromised or if the user's account management practices are weak.

5.4. Loss or Compromise of Private Keys/Seed Phrases

The fundamental security of cryptocurrency hinges on the control of private keys and seed phrases. Losing a private key or seed phrase "without a backup leads to permanent loss of access to funds". Unlike traditional financial systems, blockchain systems inherently "lack central authorities to reset passwords or recover keys". This decentralized nature, while providing autonomy, also means there is no central authority to appeal to for recovery if these critical access credentials are lost or stolen.

Poor storage practices are a primary cause of private key compromise. It is strongly advised to "Never Store Seed Phrases Digitally" in locations such as notes apps, cloud storage, or screenshots, as this "increases the risk of malware theft". Whether due to malware or careless storage, the compromise or loss of these keys results in direct and often irreversible financial loss, as the funds become inaccessible or are transferred by an attacker who gains control of the key. The core principle of crypto ownership is control over the private key. Malware can indeed steal these keys , but users themselves can inadvertently expose them through insecure storage (e.g., unencrypted files, cloud sync) or by falling for scams that trick them into revealing them. This means that even if the 721 Trojans were completely removed, if the private keys

were already compromised or poorly managed, the losses could still occur independently. This highlights the critical importance of user education on secure key management as a foundational defense against cryptocurrency loss.

6. Recommendations and Next Steps

Addressing the extensive compromise and cryptocurrency losses requires a multi-faceted approach, combining immediate remediation with long-term security enhancements and a pragmatic understanding of recovery limitations.

6.1. Immediate Actions for System Remediation

Given the scale and sophistication of the identified malware, immediate and decisive actions are paramount to prevent further losses and secure remaining assets.

- **Isolation of Infected Devices**: The laptop and any other potentially compromised devices, including the iPhone if it was connected to the laptop or used for cryptocurrency transactions, should be immediately disconnected from the internet. This action is critical to prevent further data exfiltration, lateral spread of malware, or communication with command-and-control (C2) servers.
- **Professional Malware Removal and System Re-imaging**: Self-remediation is strongly discouraged given the sheer number and complexity of the identified malware. It is highly recommended to engage a professional cybersecurity firm specializing in forensic analysis and incident response. These experts can perform a deep forensic analysis to identify all compromised areas and ensure a complete system re-imaging. Re-imaging is the most reliable way to eradicate all 721 (and potentially more) malware instances and their sophisticated persistence mechanisms, ensuring a clean slate.
- **Password Resets for All Compromised Accounts**: It must be assumed that all accounts accessed from the infected laptop or any linked devices are compromised. Passwords for *all* online accounts should be reset, with particular emphasis on cryptocurrency exchanges, digital wallets, banking services, email accounts, and social media platforms. Each account should be secured with a strong, unique password.
- **Reviewing and Securing All Cryptocurrency Wallets**:
    - Any remaining cryptocurrency funds held in hot wallets (internet-connected wallets) or on exchanges should be transferred immediately to new, secure hardware wallets (cold storage). Hardware wallets store private keys offline, significantly reducing the risk of malware-based theft.
    - For enhanced security, especially for larger holdings, the use of multi-signature (multi-sig) wallets should be considered. These wallets require multiple approvals to complete a transaction, adding a crucial layer of protection.
    - Two-factor authentication (2FA) or multi-factor authentication (MFA) must be enabled and actively used on all cryptocurrency accounts and exchanges. This adds a critical second layer of security beyond just a password.

6.2. Long-Term Security Best Practices for Cryptocurrency Holders

To prevent future cryptocurrency losses, a robust and continuous commitment to cybersecurity best practices is essential.

- **Enhanced Cyber Hygiene**:
    - Regularly update operating systems, applications, and security software (antivirus/anti-malware) on all devices. These updates often include critical security patches that address known vulnerabilities exploited by malware.
    - Use a reputable Virtual Private Network (VPN), especially when connecting to public Wi-Fi networks, to encrypt internet traffic and protect against eavesdropping and man-in-the-middle attacks.
    - Only download software from official, trusted sources. Avoid pirated software or downloads from unofficial websites, as these are common vectors for malware infection.
- **Strong Authentication**: Implement MFA/2FA on all accounts, particularly those related to cryptocurrency. Where possible, prioritize more secure second factors like hardware security keys or authenticator apps over SMS-based 2FA, which can be vulnerable to SIM swap attacks.
- **Secure Storage of Private Keys and Seed Phrases**: This is perhaps the most critical aspect of cryptocurrency security.
    - Never store private keys or seed phrases digitally on any device or cloud service. This includes notes apps, screenshots, or unencrypted files.
    - Instead, write them down on paper or engrave them on durable materials like metal plates.
    - Store multiple copies of these physical backups in different, physically secure, offline locations (e.g., a fireproof safe, a safe deposit box).
    - Regularly test these backups to ensure they are legible and can be used to recover funds if necessary.
- **Vigilance Against Phishing and Social Engineering**: Education and skepticism are powerful defenses.
    - Be highly skeptical of unsolicited emails, messages, phone calls, or investment opportunities, especially those promising high returns or requiring urgent action.
    - Always verify the URLs of legitimate websites by manually typing them or using bookmarks. Look for HTTPS and scrutinize for any spelling errors or subtle variations in domain names.
    - Never click suspicious links or open untrusted attachments in emails or messages.
    - Be aware of common scam tactics such as pig butchering, fake celebrity endorsements, and giveaway scams, which exploit psychological vulnerabilities.
- **Careful Selection of Exchanges and Platforms**: Before committing funds, thoroughly research the security measures implemented by any cryptocurrency exchange or platform. Look for features such as 2FA, cold storage for a significant portion of assets, and withdrawal whitelists.

6.3. Guidance on Engaging with Law Enforcement and Seeking Recovery

While the user has expressed frustration with past interactions, understanding the processes and limitations of law enforcement can help manage expectations for future engagement.

- **How to Report Cybercrime in the Netherlands**:
    - Advise reporting to the local police by calling 0900-8844 (within the Netherlands) or visiting a municipal police station.

    - The Fraud Help Desk can also be contacted for advice and to record reports of fraud. However, it is important to note that the Fraud Help Desk provides guidance but "has no investigative power".
    - If the scam originated from a Dutch company but the user is abroad, the report should first be made to the local police in that country, who can then liaise with the Dutch police.
- **Understanding the Limitations of Recovery**: It is crucial to set realistic expectations regarding the recovery of stolen cryptocurrency. Recovery is "extremely challenging" and often "irreversible" due to the decentralized nature of blockchain technology, the speed of transactions, and the use of obfuscation methods by criminals. Law enforcement agencies face significant hurdles in tracing and freezing funds, especially when sophisticated obfuscation methods like mixers are employed. Additionally, it is generally advised against paying ransomware demands, as there is no guarantee of file recovery, and it only serves to validate and perpetuate the criminal business model.
- **Importance of Detailed Documentation for Potential Legal Action**: For any potential investigation, however challenging, meticulous documentation is vital. This includes recording all available evidence: precise dates of loss, transaction IDs, cryptocurrency wallet addresses (both sender and receiver), communication logs with any suspicious entities or scammers, and screenshots of malware detections or other indicators of compromise. This information, even if it does not lead to immediate recovery, is crucial for law enforcement to build intelligence and potentially pursue broader criminal networks.
- **Exploring Blockchain Analytics Tools for Tracing Funds (if applicable)**: While individuals typically do not have direct access to them, it is worth noting that specialized blockchain analytics tools, such as Chainalysis, are utilized by law enforcement agencies to trace illicit funds. If stolen funds are traceable to a known, regulated exchange, there might be a slim chance of freezing them; however, this requires extremely rapid action and direct intervention by law enforcement, which is rare and highly dependent on specific circumstances.

7. Conclusion

The user's situation, marked by the identification of 721 Trojan Horse applications and years of cryptocurrency losses, represents a complex interplay of cyber threats. The analysis confirms that the identified malware list contains numerous types specifically designed to target cryptocurrency, financial credentials, and system resources. The sheer volume and diversity of these malicious programs, including sophisticated loaders and post-exploitation frameworks like Cobalt Strike, strongly indicate a prolonged and multi-vector compromise of the user's system. This persistent infection likely served as a continuous gateway for various financially motivated cybercriminal groups, directly contributing to the reported multi-year financial depletion.
While a direct assessment of the provided iPhone logs was not possible, the general risks associated with mobile malware and the potential for cross-device compromise highlight that modern cyberattacks often span multiple devices. This reinforces the need for a holistic security approach.
The perceived lack of assistance from law enforcement in the Netherlands reflects systemic challenges inherent in investigating and prosecuting cryptocurrency fraud. These include the global and decentralized nature of digital assets, jurisdictional complexities, technical and resource limitations within law enforcement agencies, and the specific mandates of financial

intelligence units that focus on intelligence rather than direct victim recovery.
Furthermore, it is critical to acknowledge that cryptocurrency losses frequently stem from sophisticated non-malware-related fraud vectors, such as high-yield investment scams, pervasive phishing attacks, and insecure practices on cryptocurrency exchanges. These often exploit human vulnerabilities or systemic weaknesses within the broader crypto ecosystem, and may have significantly contributed to, or even been the primary cause of, the user's losses, independently or in conjunction with the malware infections.
In conclusion, the user's experience is a plausible outcome of a multi-pronged attack involving direct malware infection, potentially facilitated by social engineering, and possibly compounded by broader vulnerabilities in cryptocurrency ecosystem security or investment scams. While the past cannot be undone, the future can be secured. This requires rigorous adherence to cybersecurity best practices, continuous education on emerging threats, and a pragmatic understanding of the profound challenges inherent in cryptocurrency recovery. The ultimate responsibility for securing digital assets largely falls on the individual, necessitating proactive and comprehensive security measures across all digital interactions.

Works cited

1. Lumma Infostealer Continues Its GitHub Social Engineering Campaign - Picus Security, https://www.picussecurity.com/resource/blog/lumma-infostealer-continues-its-github-social-engineering-campaign 2. Zloader Malware Analysis: Unveiling the Silent Threat in [2024] - UltraViolet Cyber, https://www.uvcyber.com/resources/reports/zloader-malware-back-in-action 3. ZLoader: What it is, how it works and how to prevent it | Malware spotlight [2022 update], https://www.infosecinstitute.com/resources/malware-analysis/zloader-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/ 4. Common Malware Loaders - ReliaQuest, https://reliaquest.com/blog/common-malware-loaders/ 5. What is Emotet Malware? Definition, infection chain and protection!, https://www.hornetsecurity.com/en/knowledge-base/emotet/ 6. Emotet Malware | CISA, https://www.cisa.gov/news-events/alerts/2018/07/20/emotet-malware 7. What is TrickBot Malware? - CrowdStrike, https://www.crowdstrike.com/en-us/cybersecurity-101/malware/trickbots/ 8. TrickBot Malware | CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-076a 9. Trojan:Win32/IcedId threat description - Microsoft Security Intelligence, https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/IcedId&threatId=-2147218071&ocid=magicti_ta_ency 10. THREAT ANALYSIS: From IcedID to Domain Compromise - Cybereason, https://www.cybereason.com/blog/threat-analysis-from-icedid-to-domain-compromise 11. Attackers Exploiting Public Cobalt Strike Profiles - Unit 42, https://unit42.paloaltonetworks.com/attackers-exploit-public-cobalt-strike-profiles/ 12. Cobalt Strike as a Threat to Healthcare - HHS.gov, https://www.hhs.gov/sites/default/files/cobalt-strike-tlpwhite.pdf 13. Lumma Stealer: Breaking down the delivery techniques and capabilities of a prolific infostealer | Microsoft Security Blog, https://www.microsoft.com/en-us/security/blog/2025/05/21/lumma-stealer-breaking-down-the-delivery-techniques-and-capabilities-of-a-prolific-infostealer/ 14. Law Enforcement Disrupts DanaBot & Lumma Stealer Malware Operations, https://www.hipaajournal.com/law-enforcement-operations-lumma-stealer-danabot/ 15. Microsoft leads international takedown of Lumma Stealer | Cybersecurity Dive, https://www.cybersecuritydive.com/news/microsoft-takedown-lumma-stealer/748727/ 16. Microsoft Identifies Remote Access Trojan Built to Drain Crypto Wallets - PaymentsJournal,

https://www.paymentsjournal.com/microsoft-identifies-remote-access-trojan-built-to-drain-crypto-wallets/ 17. StilachiRAT analysis: From system reconnaissance to cryptocurrency theft | Microsoft Security Blog, https://www.microsoft.com/en-us/security/blog/2025/03/17/stilachirat-analysis-from-system-reconnaissance-to-cryptocurrency-theft/ 18. Microsoft warns of new malware targeting cryptocurrency wallets | Digital Watch Observatory, https://dig.watch/updates/microsoft-warns-of-new-malware-targeting-cryptocurrency-wallets 19. Category deep-dive: $2.2 billion was stolen in crypto-related hacks in 2024 | TRM Blog, https://www.trmlabs.com/resources/blog/category-deep-dive-2-2-billion-was-stolen-in-crypto-related-hacks-in-2024 20. New Crocodilus malware snaps up crypto wallets - Field Effect, https://fieldeffect.com/blog/new-crocodilus-malware-snaps-up-crypto-wallets 21. Dual Malware Infection Targets Cryptocurrency Users: What You Need to Know - Cyble, https://cyble.com/blog/dual-malware-infection-targets-cryptocurrency-users/ 22. New MassJacker Malware Targets Piracy Users, Hijacking Cryptocurrency Transactions, https://thehackernews.com/2025/03/new-massjacker-malware-targets-piracy.html 23. How Clipboard Hijacking Malware Can Steal Your Crypto - OSL, https://osl.com/en/academy/article/how-clipboard-hijacking-malware-can-steal-your-crypto 24. Coinminer malware threat description - NordVPN, https://nordvpn.com/cybersecurity/threat-center/coinminer/ 25. Ransomware WannaCry: All you need to know - Kaspersky, https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry 26. WannaCry | NJCCIC - NJ.gov, https://www.cyber.nj.gov/threat-landscape/ransomware/ransomware-variants/wannacry 27. Threat description search results - Microsoft Security Intelligence, https://www.microsoft.com/en-us/wdsi/threats/threat-search?query=Snake 28. WannaCry ransomware attack - Wikipedia, https://en.wikipedia.org/wiki/WannaCry_ransomware_attack 29. What is Crypto Ransomware? - Check Point Software, https://www.checkpoint.com/cyber-hub/ransomware/what-is-crypto-ransomware/ 30. Fraud, disputes, or complaint: Who to contact? | Business.gov.nl, https://business.gov.nl/running-your-business/security-and-fraud/fraud-disputes-or-complaint-who-to-contact/ 31. What is Qakbot Malware? Definition, Detection & Removal | Darktrace, https://www.darktrace.com/cyber-ai-glossary/qakbot 32. Leader of Qakbot Malware Conspiracy Indicted for Involvement in Global Ransomware Scheme | United States Department of Justice, https://www.justice.gov/opa/pr/leader-qakbot-malware-conspiracy-indicted-involvement-global-ransomware-scheme 33. Kaspersky discovers new crypto-stealing Trojan in AppStore and Google Play, https://www.kaspersky.com/about/press-releases/kaspersky-discovers-new-crypto-stealing-trojan-in-appstore-and-google-play 34. BankBot/Spy Banker - NJCCIC - NJ.gov, https://www.cyber.nj.gov/threat-landscape/malware/trojans/bankbot-spy-banker 35. Trojan-Banker.Win32.ChePro.gen - Kaspersky Threats, https://threats.kaspersky.com/en/threat/Trojan-Banker.Win32.ChePro.gen/ 36. Trojan-Downloader.Win32.OffLoader.klr - Kaspersky Threats, https://threats.kaspersky.com/en/threat/Trojan-Downloader.Win32.OffLoader.klr/ 37. Law enforcement in the age of cryptocurrency - Police1, https://www.police1.com/investigations/law-enforcement-in-the-age-of-cryptocurrency 38. Common Challenges in Cybercrime 2024 - Europol, https://www.europol.europa.eu/cms/sites/default/files/documents/Common_Challenges_in_Cybercrime_2024.pdf 39. Crypto is soaring, but so are threats: Here's how to keep your wallet safe -

WeLiveSecurity,
https://www.welivesecurity.com/en/cybersecurity/crypto-soaring-threats-how-keep-wallet-safe/
40. Crypto Security and its Importance - A Complete Guide,
https://www.tokenmetrics.com/blog/crypto-security 41. Cryptocurrency hacks and thefts:
Insecure exchanges?: Constangy Cyber Advisor,
https://www.constangy.com/constangy-cyber-advisor/cryptocurrency-hacks-and-thefts-insecure-exchanges 42. FIU-the Netherlands, https://www.fiu-nederland.nl/en/ 43. What is
FIU-Netherlands? - Sanction Scanner,
https://www.sanctionscanner.com/knowledge-base/financial-intelligence-unit-the-netherlands-354 44. Common Challenges in Cybercrime | Europol - European Union,
https://www.europol.europa.eu/publications-events/publications/common-challenges-in-cybercrime 45. 2025 Crypto Crime Trends from Chainalysis,
https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/ 46. What Is a Phishing
Attack in Crypto, and How to Prevent It? - OSL,
https://www.osl.com/hk-en/academy/article/what-is-a-phishing-attack-in-crypto-and-how-to-prevent-it 47. Cryptocurrency Scams - NJCCIC - NJ.gov,
https://www.cyber.nj.gov/threat-landscape/phishing-online-scams/cryptocurrency-scams 48.
How To Avoid Cryptocurrency Scams - Kaspersky,
https://usa.kaspersky.com/resource-center/definitions/cryptocurrency-scams 49. What To Know
About Cryptocurrency and Scams - Federal Trade Commission,
https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams 50. What Happens
if You Lose Your Private Key? Lessons From High-Profile Hacks - CCN.com,
https://www.ccn.com/education/crypto/lose-private-key-crypto-hacks-examples/ 51. Private Key
Recovery: What To Do When You Forget Your Crypto Access - CCN.com,
https://www.ccn.com/education/crypto/private-key-recovery-best-practices/ 52. This Malicious
PyPI Package Stole Ethereum Private Keys via Polygon RPC Transactions,
https://thehackernews.com/2025/03/this-malicious-pypi-package-stole.html